

**ENTERED**

April 13, 2017

David J. Bradley, Clerk

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF TEXAS  
CORPUS CHRISTI DIVISION

UNITED STATES OF AMERICA	§	
	§	
VS.	§	CRIMINAL ACTION NO. 2:16-CR-928
	§	
HENRY FRANKLIN REDDICK	§	

**ORDER ON MOTION TO SUPPRESS**

Defendant Henry Franklin Reddick (Reddick) is charged by indictment with four counts of possession of child pornography. D.E. 1. Before the Court is his motion to suppress evidence (D.E. 34). First, he seeks to exclude all of the alleged images of child pornography that a private party referred—in unopened electronic files—to law enforcement. His reasoning is that the officer engaged in a search beyond the scope of the private party's investigation by opening and viewing the contents of those electronic files without a warrant (Phase I search). Second, he seeks to exclude all evidence found in his home and on his computer because the search warrant used to search his property (Phase II search) was based, in part, on the information gleaned from the initial warrantless viewing.

The Government argues that it did not engage in an unreasonable search and seizure because its Phase I search did not exceed the scope of the private investigation and referral. Alternatively, the Government argues that if it exceeded the scope of the private search, the good faith exception to the exclusionary rule permits admission of the evidence the officers found when executing what they believed was a valid search warrant. D.E. 36, 41. Reddick responds that the Phase I search exceeded the scope of

any private search and the officer's conduct in securing the Phase II search warrant takes it outside the good faith exception to the exclusionary rule. D.E. 40.<sup>1</sup> For the reasons set out below, the Court DENIES the motion to suppress.

## FACTS

PhotoDNA is a software program using an algorithm by which still and video digital images are converted to grayscale, broken down into grids of data, and assigned certain alphanumeric values associated with the hue gradient of the target material, arriving at what is called a "hash value." The hash value has been described as an electronic equivalent of a fingerprint<sup>2</sup> in that two iterations of the same image will, to an over 99% level of accuracy, produce the same hash value.<sup>3</sup> Conversely, the chances of two different images generating the same hash value is nearly non-existent.

Some of the advantages to using the PhotoDNA software include the ability to scan large numbers of electronic files for their hash values in very little time, and doing so without exposing the images to viewers. The software thus ferrets out child pornography and protects children from additional exploitation. While hash values are useful and reliable for identifying matches to known images, one cannot recreate an image or determine its content solely from its hash value. Therefore, without viewing the

---

<sup>1</sup> Reddick also argues that there were no exigent circumstances to support a warrantless search. The Government does not rely on any exigent circumstances exception to the warrant requirement, making this issue moot.

<sup>2</sup> *United States v. Chiaradio*, 684 F.3d 265, 271 (1st Cir. 2012). *See also United States v. Farlow*, 681 F.3d 15, 19 (1st Cir. 2012); *United States v. Cunningham*, 694 F.3d 372, 376 n.3 (3rd Cir. 2012); *United States v. Miknevich*, 638 F.3d 178, 181 n.1 (3rd Cir. 2011); *United States v. Richardson*, 607 F.3d 357, 363 (4th Cir. 2010); *United States v. Dodson*, 960 F.Supp.2d 689, 692 n.1 (W.D. Tex. 2013).

<sup>3</sup> *See generally, United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012). *See also United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (in challenge to probable cause supporting search warrant, rejecting argument "that it is possible for two digital files to have hash values that collide or overlap").

electronic image or the material from which the matching hash value was sourced, one cannot say with certainty that the electronic file is, in fact, contraband. The high likelihood that it is contraband stems from the integrity of the database of offending hash values used to test for matches.

With the imprimatur of the federal government,<sup>4</sup> the National Center for Missing and Exploited Children (NCMEC) established a database containing the hash values of known images that contain confirmed or suspected child pornography. There are multiple contributors to the database and, on this record, it is uncertain what criteria govern and whose judgment is used when a particular hash value result is included in the NCMEC database. And, because the original images from which offending hash values were generated are destroyed, there is no readily available matching image to view to confirm the illegal nature of a matched hash value image.

Reddick submits that the judgment call used to populate the NCMEC database may lead to adult pornography being submitted erroneously as child pornography or there may be contributions that cause other false positives in searching for contraband. D.E. 40, p. 2 n.1 (citing a New York Post article regarding one such misidentification of an adult as a child). However, there is no evidence that such over-inclusiveness has occurred in the NCMEC database or is widespread, impugning the overall integrity of the database. Instead, law enforcement regularly relies on a hash value match with the

---

<sup>4</sup> The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 et seq., created rules to guarantee electronic privacy. In its Title II, the Stored Communications Act (SCA), Congress prescribed the circumstances under which the government may compel disclosure or when service providers may voluntarily disclose a customer's communications or records. Under that statute, a provider must report apparent child pornography to NCMEC via its Cyber Tipline if the provider becomes aware of it. 18 U.S.C. § 2258A.

NCMEC database results to successfully identify images that are, indeed, images of child pornography.

Many internet service providers, desiring to avoid any reputation for aiding those who possess or transmit child pornography, use PhotoDNA to scan files that customers upload through the service providers' browsers, applications, or cloud storage facilities. They then compare the hash value results with the hash values in the NCMEC database. When they get a match, they refer the files, along with subscriber information, to NCMEC as required by law. NCMEC, without opening the electronic file, generates a report and conducts an initial investigation, limited to confirming the hash value match and identifying the location of the internet user whose equipment uploaded the matching file. NCMEC then forwards the report (CyberTipline report) to the appropriate law enforcement agency with geographic jurisdiction over the internet user for further investigation.

Reddick made use of software systems that stored his electronic files in a cloud maintained by Microsoft Corporation and referred to as Skydrive. At the suppression hearing, Reddick did not offer evidence of any terms on which his files were so maintained. The Government offered the standard end user agreement of Microsoft OneDrive for that purpose. While OneDrive is the current electronic system formerly referred to as Skydrive, the Government's witnesses could not testify that the current OneDrive agreement stated the same terms that were in place when the events of this case transpired—during the Skydrive period. The Court therefore excluded the OneDrive agreement from evidence. While the Government's witnesses then testified that there is a

standard in the industry by which privacy rights are waived in cloud storage agreements, permitting PhotoDNA scans and law enforcement referrals, they were not able to opine that the specific agreement governing Reddick's account met that standard.

At any rate, Microsoft Skydrive conducted a hash value examination of electronic files on its system, including those related to Reddick. Several of Reddick's files generated hash values that matched hash values in the NCMEC database. As required by law, Microsoft Skydrive copied the electronic files and referred them to NCMEC, along with Reddick's subscriber information and other metadata that identified when and how the files were uploaded. NCMEC determined that Reddick was within the jurisdiction of Corpus Christi, Texas.

On March 10, 2015, the Corpus Christi Police Department (CCPD) Organized Crime Unit–Internet Crimes Against Children (ICAC) Task Force received three CyberTipline reports from NCMEC, containing 13, 50, and 16 electronic files, respectively. The NCMEC transmission of the files to CCPD-ICAC included the assertion that the files had been hash value matched, but had not been opened or viewed. Officer Michael Ilse, a CCPD-ICAC member, received the reports and opened and viewed the contents of the files (Phase I search) to confirm that the images depicted child pornography. He testified that he always visually confirms that the files contain child pornography before seeking a search warrant and that this is the established practice of all detectives he knows who investigate these crimes.

Officer Ilse then submitted an affidavit with a request for a search warrant to search and seize Reddick's computer and related materials (Phase II search). In his

5 / 14

affidavit, among other things, he recounts the NCMEC CyberTipline reports, describes the matching of hash values, lists some of the file names,<sup>5</sup> and recites that he opened and viewed the files, stating why they appear to contain child pornography. A state district judge issued the warrant on April 9, 2015. CCPD searched Reddick's residence, including several digital devices, and found evidence of child pornography, including 456 still images and 13 videos. Nine of those files matched those transmitted to CCPD in the NCMEC CyberTipline reports. Reddick was later arrested on November 10, 2016.

## **DISCUSSION**

### **A. Burden of Proof**

Reddick asserts that Officer Ilse's review of the files uploaded to Skydrive (Phase I search) was a warrantless search in violation of the Fourth Amendment. And because the subsequent Phase II search was conducted pursuant to a warrant that was based on information accessed through the Phase I warrantless search, the evidence obtained is fruit of the poisonous tree. Accordingly, all evidence obtained as a result of the Phase I warrantless search of the files uploaded to Skydrive must be suppressed. D.E. 34, p. 2.

**Unconstitutional Search.** It is the defendant's burden to prove a Fourth Amendment violation by a preponderance of the evidence. *United States v. Riazco*, 91 F.3d 752, 754 (5th Cir. 1996). To show a Fourth Amendment violation, a defendant must first establish that the search invaded a legitimate expectation of privacy that society recognizes as reasonable. *See generally, Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990)

---

<sup>5</sup> Along with some file names that are simply alphanumeric strings, there were files labeled: sucking mandick.jpg, very yb and dad.jpg, boy sucking boydick.jpg, boydick and mancock.jpg, boy.kiddy.pedo.Sebastian Bleisch – Das Lagerhaus – 4 ET (gay preteen kidsex) 9.06.mpg. Government Exhibit 2.

(quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)). Whether the search was a reasonable intrusion into that privacy interest depends on whether the government acted pursuant to a warrant. A warrantless search is presumed unreasonable and shifts the burden of proof to the government to establish an exception to the warrant requirement. *United States v. Castro*, 166 F.3d 728, 733 n. 7 (5th Cir. 1999) (en banc); *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005). Such exceptions include special law enforcement needs, exigent circumstances, diminished expectations of privacy, and minimal intrusions. *See generally, Illinois v. McArthur*, 531 U.S. 326, 330 (2001).

**Exclusionary Rule.** If the evidence supports a finding of an unconstitutional search, there is a presumption that the resulting evidence should be excluded from the trial. Thus, the burden is on the government to demonstrate why the exclusionary rule should not apply to the fruits of the illegal search or seizure. *United States v. Houltin*, 566 F.2d 1027, 1031 (5th Cir. 1978). *See also, United States v. Runyan*, 275 F.3d 449, 456 (5th Cir. 2001). One such reason is that the search was conducted in good faith reliance on a warrant thought to be valid. *United States v. Leon*, 468 U.S. 897, 926 (1984).

#### **B. On this Record, the Court Assumes an Unlawful Search**

According to the Fifth Circuit, the relevant factors for a determination of a reasonable expectation of privacy are: (1) whether the defendant has a property or possessory interest in the thing seized or the place searched; (2) whether he has the right to exclude others from the place; (3) whether he has exhibited a subjective expectation of privacy that it would remain free from governmental intrusion; (4) whether he took

7 / 14

normal precautions to maintain privacy; and (5) whether he was legitimately on the premises. *United States v. Runyan*, 275 F.3d 449, 457 (2001) (quoting *United States v. Cardoza-Hinojosa*, 140 F.3d 610, 615 (5th Cir. 1998)). “[T]he *Cardoza-Hinojosa* factors, ‘while appropriate to determine the expectation of privacy in the context of searches of physical real property,’ cannot necessarily be applied to other types of searches without modification.” *Id.* (quoting *Kee v. City of Rowlett, Texas*, 247 F.3d 206, 212-13 (5th Cir. 2001)).

The expectation of privacy in this digital age is fraught with varying levels of confidence in the ability to protect electronic data as well as specialized needs to monitor data systems for electronic viruses, hacking attempts, phishing efforts, malware, illegal content, international security, and other threats. One’s expectation of privacy is no easy issue in the abstract and the parties have deprived the Court of the most useful evidence on which to make the determination in this case—the end user agreement governing Reddick’s use of Microsoft Skydrive. That agreement, by which the user’s electronic data is stored on a private system, ordinarily specifies who may access the data, how that data may be accessed, and for what purposes. Only with that information could the Court reliably begin to address whether Reddick had a constitutional expectation of privacy or had waived any such expectation by contractually permitting searches for contraband images.

The privacy issue, while starting with an end user agreement, would not necessarily end there. The Court would have to make other technology-specific determinations involving undeveloped facts and law with respect to the issues of the

8 / 14



scope of the private search, the significance of the algorithmic “view” of the file, and any remaining expectation of privacy after a NCMEC database match is discovered. For instance:

- Is an electronic file already searched if its contents are invaded for the purpose of determining its hash value?<sup>6</sup>
- Does law enforcement gain any material information it did not already know by opening an electronic file that has already been hashed and matched?<sup>7</sup>
- Is the slight possibility that viewing the file will expose an image that is not contraband within social tolerances?
- Is viewing a file a new search when an exact copy of the file was opened by someone else and reported to NCMEC as child pornography, causing its hash value to be added to the NCMEC database?<sup>8</sup>
- Would it make a difference if the government used the hash value only for purposes of matching and viewed only a separate copy of the matched image that had been stored or was located elsewhere outside of the defendant’s possession?

---

<sup>6</sup> “[A] police view subsequent to a search conducted by private citizens does not constitute a ‘search’ within the meaning of the Fourth Amendment so long as the view is confined to the scope and product of the initial search.” *United States v. Bomengo*, 580 F.2d 173, 175 (5th Cir.1978); *see also United States v. Paige*, 136 F.3d 1012, 1019 (5th Cir.1998). At least one court has held that hash value analyses do constitute searches for Fourth Amendment purposes. *See United States v. Crist*, 627 F. Supp. 2d 575, 585 (2008) (“The Court rejects [the Government’s] view and finds that the ‘running of hash values’ is a search protected by the Fourth Amendment.”); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) (“[T]he government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools should not be used without specific authorization in [a] warrant.”). However, some commentators have argued that because of the non-intrusive nature of hash value analyses and their ability to discern contraband without revealing other content, they should not be considered searches under the Fourth Amendment. These commentators have concluded that hash value comparisons are analogous to a canine sniff. *See* Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 Geo. Mason. L. Rev. 255, 276-80 (2011); Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 44-46 (2005).

<sup>7</sup> Where law enforcement’s search only confirms what it already knew with substantial certainty, it does not expand the scope of a private search. *United States v. Runyan*, 275 F.3d at 463.

<sup>8</sup> Actions that “enabled the agent to learn nothing that had not previously been learned during the private search” do not invade a legitimate expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 127 (1984).

- Is the NCMEC database of hash values sufficiently reliable to equate a match with a contraband image?
- If there is no constitutional expectation of privacy in contraband, does opening an isolated electronic file implicate anything more than what the hash value has indicated to be contraband, akin to a field test of controlled substances?<sup>9</sup>

There are cases that have addressed some of these issues, but they are not all consistent. And the Fifth Circuit has not yet issued opinions to provide this Court with guidance regarding these very specific technology-and policy-intense matters.

As will be demonstrated below, the evidence here supports the good faith exception to the exclusionary rule. For this reason, the Court declines to wade into the myriad of issues regarding Reddick's expectation of privacy. The Court will assume without deciding that Officer Ilse's viewing of the file images (Phase I search) invaded a constitutional expectation of privacy, exceeded the scope of Microsoft Skydrive's hash value search, and did not fall into any exception to the warrant requirement.

### **C. The Good Faith Exception to the Exclusionary Rule Applies**

The exclusionary rule is a remedy imposed to protect the Fourth Amendment by suppressing evidence obtained through an illegal search. *United States v. Leon*, 468 U.S. 897, 906 (1984)). The derivative evidence rule, also known as the fruit of the poisonous tree doctrine, further requires suppression of evidence that is discovered as an indirect result of police misconduct. *United States v. Tedford*, 875 F.2d 446, 450 (5th Cir. 1989).

---

<sup>9</sup> "No protected privacy interest remains in contraband in a container once government officers lawfully have opened that container and identified its contents as illegal. *Illinois v. Andreas*, 463 U.S. 765, 771 (1983). "[G]overnmental conduct that only reveals the possession of contraband 'compromises no legitimate privacy interest.'" *Illinois v. Caballes*, 543 U.S. 405, 408 (2005).

There are four recognized exceptions<sup>10</sup> to these rules. The Government relies only upon the good faith exception, allowing admission of evidence obtained in good faith reliance upon a warrant that is found invalid after its execution.

In *Leon*, the Court reasoned that excluding evidence when law enforcement acted in good faith on a warrant would not further the purpose of the exclusionary rule: to deter unconstitutional conduct. “Penalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of the Fourth Amendment violations.” *Leon*, 468 U.S. at 921. Thus, “In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.”<sup>11</sup> *Id.* at 926. “[T]he analysis ‘is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s

---

<sup>10</sup> The exceptions are: (1) dissipated taint: when “the connection between the illegal police conduct and the discovery and seizure of the evidence is ‘so attenuated as to dissipate the taint;’” (2) independent source: when the evidence was discovered by means wholly independent of the constitutional violation, even if the same evidence was also discovered during or as a consequence of illegal police conduct; (3) Inevitable discovery: when the evidence would have been discovered by lawful means had the investigation continued without the tainted evidence; and (4) good faith: when law enforcement reasonably relied in good faith upon a warrant later found to be improperly issued. While the hash value match to the NCMEC database and some of the file names might have justified using the fruits of the Phase II search under the independent source or inevitable discovery rules, the Government did not plead those exceptions. *United States v. Ceccolini*, 435 U.S. 268, 279 (1978) (first exception); *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (second exception); *Brewer v. Williams*, 430 U.S. 387, 406 n. 12 (1977) (third exception); *United States v. Leon*, 468 U.S. 897, 924 (1984) (fourth exception).

<sup>11</sup> The Fifth Circuit has acknowledged that the good faith exception will not apply in four scenarios: (1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; (2) when the issuing magistrate wholly abandoned his judicial role; (3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and (4) when the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers cannot reasonably presume it to be valid. *Massi*, 761 F.3d at 529-30 (quoting *United States v. Woerner*, 709 F.3d 527, 533-34 (5th Cir. 2013)).

authorization.”” *United States v. Massi*, 761 F.3d 512, 530 (5th Cir. 2014) (citing *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003)).

Reddick argues that the good faith exception does not apply because Officer Ilse knew or should have known that his Phase I search was illegal and he only perpetuated his illegal conduct by securing a Phase II search warrant based on that illegal Phase I search. The Fifth Circuit has resolved that issue in favor of law enforcement, making the test whether the illegal search was a close call: “the prior law enforcement conduct that uncovered evidence used in the affidavit for the warrant must be ‘close enough to the line of validity’ that an objectively reasonable officer preparing the affidavit or executing the warrant would believe that the information supporting the warrant was not tainted by unconstitutional conduct . . . .” *Massi*, at 528.<sup>12</sup>

The Fifth Circuit has not had many opportunities to explain what sort of conduct is “close enough to the line of validity” so as to warrant application of the good faith exception.<sup>13</sup> However, given the issues in this case, the Court finds that Officer Ilse’s search qualifies. As apparent from the discussion above, the Phase I search issues involve unclear boundaries on electronic data privacy interests and the significance of the prior—private—hash value invasion of files and NCMEC database matching. And this

---

<sup>12</sup> See also, *United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005). But cf., *United States v. McGough*, 412 F.3d 1232, 1239-40 (11th Cir. 2005) (good faith exception does not apply where a search warrant is issued on the basis of evidence obtained as the result of an illegal search); *United States v. Vasey*, 834 F.2d 782, 789-90 (9th Cir. 1987) (magistrate’s issuance of warrant based on tainted evidence does not sanitize the taint).

<sup>13</sup> In *Massi*, the court held that a warrant issued after a prolonged detention that was not supported by reasonable suspicion or probable cause fell within the good faith exception because of “the absence of precedent on holding suspects and their ‘vehicle’ in order to prepare a proper warrant request, as opposed just to searching under exigent circumstances without a warrant.” *Massi*, 761 F.3d at 529. In another case, the court held that a dog sniff of the defendant’s garage door was “close enough to the line of validity” for purposes of the good faith exception. *United States v. Holley*, 831 F.3d 322, 327 (5th Cir. 2016).

record reflects the near certainty that the electronic files were each single images that qualified as child pornography: contraband and nothing more.

Most telling on the issue of good faith is the fact that, in his affidavit seeking a search warrant, Officer Ilse fully recited the circumstances by which he came into possession of the Phase I files and the fact that he opened them and viewed them. This exhibits a firmly held conviction that his Phase I investigation, including viewing of the files, was appropriate and lawful. Had it not been, he would have reason to expect that the judge issuing the search warrant would tell him and refuse to issue the Phase II search warrant.

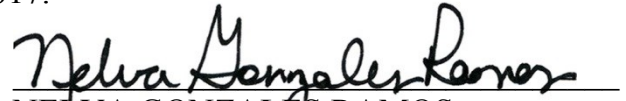
The Court finds that Officer Ilse's reliance on the warrant was objectively reasonable. There was nothing in the warrant or otherwise known by him that would have made an objectively reasonable officer doubt the warrant's validity. Furthermore, there is no evidence in the record to indicate that any of the disqualifying scenarios, involving dishonest or misleading police conduct or the magistrate judge's abandonment of his or her role as independent arbiter are applicable to this case. Indeed, the NCMEC match and file names, without viewing the images, might establish sufficient probable cause to support the validity of the warrant. *See United States v. Cartier*, 543 F.3d at 446 (stating that a hash value match from a reliable source could support the issuance of a warrant under the totality of the circumstances). Thus, the good faith exception applies.

## **CONCLUSION**

Assuming without deciding that there was an unconstitutional Phase I search and that the resulting search warrant was infirm, the Court finds that the Phase II search was

accomplished in good faith reliance on a warrant with apparent validity. Suppressing the evidence would not further the purposes of the exclusionary rule. Accordingly, Reddick's motion to suppress (D.E. 34) is DENIED.

ORDERED this 13th day of April, 2017.

  
NELVA GONZALES RAMOS  
UNITED STATES DISTRICT JUDGE